



GUNNISON, MCKAY & HODGSON, L.L.P. AF/IFW
GARDEN WEST OFFICE PLAZA, SUITE 220
1900 GARDEN ROAD
MONTEREY, CALIFORNIA 93940
(831) 655-0880
FACSIMILE (831) 655-0888

October 28, 2008

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL LETTER FOR REPLY BRIEF

RE: Applicant(s): Eduard K. de Jong

Assignee: Sun Microsystems, Inc.

Title: RENDERING AND ENCRYPTION ENGINE FOR
APPLICATION PROGRAM OBFUSCATION

Serial No.: 10/672,184 Filed: September 25, 2003

Examiner: Ponnoreay Pich Group Art 2135
Unit:

Docket No.: SUN040027

Dear Sir:

Transmitted herewith are the following documents in
response to the Examiner's Answer dated August 29, 2008 in the
above application:

1. Return receipt postcard;
2. This Transmittal Letter (2 pages); and
3. Reply Brief (12 pages); and

Conditional Petition for Extension of Time: If an
extension of time is required for timely filing of the
enclosed documents after all papers filed with this
transmittal have been considered, Applicant(s) hereby petition
for such an extension of time.

Transmittal Letter
Serial No. 10/672,184
October 28, 2008

The Commissioner is hereby authorized to charge any additional fees required for consideration of the enclosed documents, and to credit any overpayment of fees to Deposit Account No. 50-0553.

CERTIFICATE OF MAILING

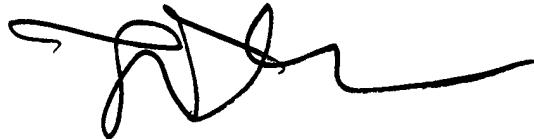
I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on October 28, 2008.



Attorney for Applicant(s)

October 28, 2008
Date of Signature

Respectfully submitted,



Forrest Gunnison
Attorney for Applicant(s)
Reg. No. 32,899

Serial No. 10/672,184
Examiner's Answer Dated: August 29, 2008
Reply Brief Filed: October 28, 2008

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Eduard K. de Jong

Assignee: Sun Microsystems, Inc.

Title: RENDERING AND ENCRYPTION ENGINE FOR APPLICATION
PROGRAM OBFUSCATION

Serial No.: 10/672,184 Filed: September 25, 2003

Examiner: Ponnoreay Pich Group Art
Unit: 2135

Docket No.: SUN040027

Monterey, CA
October 28, 2008

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY BRIEF

Dear Sir:

Pursuant to 37 CFR § 41.41, Appellant files this Reply Brief in response to the Examiner's Answer dated August 29, 2008.

Serial No. 10/672,184
Examiner's Answer Dated: August 29, 2008
Reply Brief Filed: October 28, 2008

STATUS OF CLAIMS

Claims 1 to 20 are pending. Claims 1 to 4, 6 to 9, 11 to 14 and 16 to 19 stand rejected in the Final Office Action of November 26, 2007. Claims 5, 10, 15 and 20 stand withdrawn in the Final Office Action of November 26, 2007. The rejections of Claims 1 to 4, 6 to 9, 11 to 14 and 16 to 19 has been appealed.

Serial No. 10/672,184
Examiner's Answer Dated: August 29, 2008
Reply Brief Filed: October 28, 2008

GROUNDSD OF REJECTION TO BE REVIEWED ON APPEAL

1. Whether Claims 1 to 4, 6 to 9, 11 to 14 and 16 to 19 are unpatentable under 35 U.S.C. § 103(a) over U. S. Patent No. 7,170,999, in view of U.S. Patent No. 6,789,177, further in view of PCT Publication No. WO 02/079955, and still further in view of U.S. Patent Application Publication No. US 2002/0120854 A1?

ARGUMENT

Claims 1, 6, 11 and 16 are patentable.

The Examiner's Answer continues the misinterpretations and mischaracterizations of the references and makes the claim that Appellant's remarks are misdirected. The Examiner's Answer asserts that Appellant's remarks are without evidence and are simply argument; are presented for a first time and so should not be considered; and are considering the references in isolation.

The evidence in the present appeal is the cited prior art references, as interpreted by one of skill in the art, and Appellant's disclosure. The MPEP requires that in an obviousness rejection, the prior art references must be considered as a whole. MPEP § 2141.02 I., 8th Ed. Rev. 6, p 2100-123 (Sept. 2007).

The Examiner's Answer continues to use Appellant's claim language as a road map to identify pieces with names similar to elements in the claims and extract and re-arrange those elements without regard to the teachings of the references taken as a whole. The MPEP specifically provides that this use of hindsight is impermissible.

At page 29, the Examiner's Answer mischaracterizes Appellant's Arguments and Okada.

The Examiner's Answer, as quoted below, selectively extracted the session keys from Okada without considering Okada as a whole. With respect to the initial encryption of the contents key, Okada describes more is needed than just the use of a session key to provide adequate security. At Col. 9, lines 22 to 26, Okada describes that the contents key is not encrypted just using a session key, but rather "with a host ID

Serial No. 10/672,184
Examiner's Answer Dated: August 29, 2008
Reply Brief Filed: October 28, 2008

...., the session key and the first drive ID of the drive 100." Thus, three elements are used in the encryption.

However, this section does not explain how the encryption is done by Okada. The way that the encryption is done is described, for example, at Col. 12, lines 25 to 35. Thus, contrary to the statements in the Examiner's Answer, the encryption of Okada utilizes multiple elements and not just a session key and in particular as shown in Fig. 1 utilizes a host key and a drive key with elements 245 and 246. When Okada is considered as whole, Col. 9, line 22 to 26 cannot be read in isolation as was done in the rejection, but rather must be read in terms of how Okada teaches the actual encryption is done.

With respect to the teaching of Okada on how the encrypted contents key is decrypted, consider Fig. 1 of Okada. Fig. 1 shows that a decryption unit 271 receives the encrypted contents key from a transfer section 143 and also receives a drive key. Decryption section 271 provides an input to decryption section 272 that also receives a host key as an input. The output of section 272 is a decrypted contents key. This gives an overview of the decryption process taught by Okada and explicitly shows that a drive key and a host key are used in that process. Thus, Okada shows that two decryption sections 271, 272, a drive key and a host key are needed to obtain a decrypted contents key.

The operation of decryption sections 271, and 272 with respect to the drive key and the host key to obtain the decrypted contents key is described at Okada, Col. 10, lines 39 to 44, which stated:

The decryption section 271 decrypts the encrypted contents key read out from the storage section 150 (key file 151) of the drive 100 using the drive key (equivalent) from the encryption section 242. The decryption section 272 further decrypts the decryption result by the decryption section 271 using the host key from the encryption section 244.

Okada uses decryption section 271 to decrypt "the encrypted contents key" using the drive key as shown in Fig. 1.

The output from decryption section 271 is provided to decryption section 272 that uses the host key to generate the decrypted contents key as shown in Fig. 1. Thus, this section of Okada expressly describes how the decrypted contents key is obtained starting with the encrypted contents key using the host key and the drive key, which are the same keys that were used in the encryption process also as shown in Fig 1.

Col. 9, lines 44 to 46, Okada describes that the drive key is generated using the session keys to encrypt the first drive ID. The session keys and first drive ID are stored in RAM 210 of Okada.

At Col. 10, lines 8 to 10, Okada described that the host key is generated using the host ID and the session keys. The host ID is described as stored in ROM 220 of Okada.

Thus, the above quoted description from Okada, Col. 10, lines 39 to 44 teaches that decryption sections 271, 272 function as a decrypting means for the encrypted contents key. The use of the drive key and the host key establishes that the session keys and first drive ID stored in RAM 210 and the host ID stored in ROM 220 are used. This all follows directly from the above quoted section of Okada.

Okada also taught that before the decryption is done, an authentication must be performed. Thus, at Col. 10, lines 45 to 53, Okada first described the condition that must be satisfied to perform the decryption of the encrypted contents key (the authentication), and then summarized the decryption based on the teaching of Col. 10, lines 39 to 44. The summary at Col. 10 lines 47 to 54 of Okada is equivalent to the immediately preceding paragraph.

Thus, Okada expressly described that the encrypted contents key is encrypted using more than a session key, which

is ignored in the Examiner's Answer. Also, the Examiner's Answer demonstrates that Okada was not considered as a whole by stating:

What appellant has done is point to one section of Okada which discusses use of a session key (along with other keys) used to encrypt the contents key (col 9, lines 22-26), then point to another section (col 10, lines 39-42) which doesn't have anything to do with decryption to undo the encryption done with the session key discussed in column 9, lines 22. This sort of analysis of Okada by appellant is about as useful and just as ridiculous as if someone were to point to a section of Okada which discusses encryption and then point to just Okada's patent number and then say "clearly Okada only teaches encryption, but not decryption since the patent number doesn't say anything about decryption". As evidenced by the above portions of Okada cited by the examiner, Okada does in fact teach encryption of a contents key using a session key and decryption of the encrypted contents key using the same session key. The portion cited by appellant (col 10, lines 39-42) which discusses decryption of the session key using a drive key is to undo encryption using the drive key as discusses in column 9, lines 47-50, not decryption to undo the encryption of the contents keys that was encrypted using the session key as discussed in column 9, lines 22-26. It was appellant who mischaracterized Okada's teachings, not the examiner. Clearly appellant has failed to consider the reference as a whole since appellant so severely mischaracterized Okada's teachings.
(Emphasis Added.)

Examiner's Answer, pg. 29

The analysis of Okada demonstrates that the above comments from the Examiner's Answer have no merit and mischaracterize both Okada and Appellant's position. As demonstrated above, Col. 10, line 39 stated "decrypts the encrypted contents key."

This is not decryption of the session key as stated in the above quote from the Examiner's Answer. Appellant demonstrated above that in fact the interpretation in Appellant's Brief is correct. Vehemently asserting an incorrect position does not make the position correct when the position is directly contradicted by the reference taken as a whole.

Serial No. 10/672,184
Examiner's Answer Dated: August 29, 2008
Reply Brief Filed: October 28, 2008

The above quotation from the Examiner's Answer demonstrates that Okada was not considered as a whole. Okada teaches a process that is fundamentally different from that relied upon in the rejection and Okada provides no support for simply extracting one piece, session keys, and using that piece in a way different than that taught by Okada. This alone is sufficient to overcome the obviousness rejection.

The Examiner's Answer at pages 9, 14, 23, 36, 37 takes the position that information in Appellant's Brief should be ignored because the information allegedly is presented for the first time in the Brief. Appellant points out the Rules specifically provide when grounds for overcoming the rejection will not be considered on Appeal. Specifically,

Any arguments or authorities not included in the brief or a reply brief filed pursuant to § 41.41 will be refused consideration by the Board, unless good cause is shown.

37 C.F.R. § 41.37(vii), October 2008.

The rules could have stated that any arguments not presented in office action responses will not be considered on Appeal, but the rules do not state such a limitation. Rather, the rules specifically provide that the Appeal Brief taken with the Reply Brief establish the point for drawing the line on what may be considered on appeal. The Examiner's Answer attempts to impose a different standard.

The rules provide specific direction on what can be considered on Appeal and the rules do not support the Examiner's position. Moreover, the new rules that come into effect on December 10, 2008 specifically contemplate that grounds may be raised for the first time on appeal and so make explicit that which is implicit in the above quoted existing rule. See § 41.37 (o), U.S. Patent and Trademark Office, 1332 OG 125, July 1, 2008. Accordingly, Appellant respectfully

Serial No. 10/672,184
Examiner's Answer Dated: August 29, 2008
Reply Brief Filed: October 28, 2008

submits that all issues raised in the Appeal Brief should be considered.

As noted above, the Examiner's Answer fails to consider the references as a whole and attacks Appellant's Brief for performing such a consideration. The positions taken in the Examiner's Answer appear to ignore that each prior art reference teaches a particular type of encryption and the sequence of operations that are needed to provide the desired security using such encryption. Neither the rejection nor the Examiner's Answer has cited any teaching that pieces can be extracted from different encryption processes and then used and recombined in a completely different encryption process. The Examiner's Answer interjects proposed alternatives, without consideration as to what either reference taught and then tries to reduce the consideration of the explicit teachings of the reference to being just arguments of counsel. This is yet a further indication that the references have not been considered as a whole.

Both Kessler and Okada taught that in the encryption process, it was necessary to use keys that were associated with a particular entity. The host and drive keys of Okada were considered above. Kessler taught:

The client software includes a unique secret key, SK, and a unique public key, PK, for each registered client computer.

Kessler, Col. 4, lines 46 to 48. Thus, Kessler taught that unique keys were required for each registered client computer. To interpret Kessler otherwise negates the above quoted teaching of Kessler and so changes the principles of Kessler.

Similarly, Okada, as discussed above, used a host ID and a first drive ID in the encryption process along with the session keys to generate two different keys that were taught as required in both the encryption and decryption processes. Both

Serial No. 10/672,184
Examiner's Answer Dated: August 29, 2008
Reply Brief Filed: October 28, 2008

of the host ID and the first drive ID of Okada are associated with hardware entities, just as the unique public and secret keys were associated with each registered client computer of Kessler.

The Examiner's Answer, at pages 30 to 38 for example, proposes to justify replacing the public/private key pair in Kessler with a session key. However, both prior art references demonstrate that this is unacceptable.

Accordingly, the proposed modification of Kessler using Okada not only ignores what each reference teaches is needed with respect to the keys used in encryption, but also changes the principles of Kessler by eliminating the unique public/private keys and using a session key that Okada establishes is insufficient by itself for secure encryption. In the alternative, the Examiner's Answer purports to use a user id and password, but has failed to cite any evidence of use of such elements in encryption in the references relied upon. The user id and password are fundamentally different because they are associated with the end user and not the hardware as stated in the two references. In both references, hardware elements are associated with the two keys used. Thus, the proposed modification changes the principles of both prior art references and so is inappropriate. MPEP §2143.01 VI., 8th Ed., Rev. 6, pg. 2100-141, (Sept. 2007).

The Examiner's Answer asserts that such a change does not change the principles of Kessler. However, if arbitrarily extracting pieces from Kessler and Okada and using them in a way different than taught by either reference and in a way that directly contradicts the teachings of Kessler and Okada, replacing private/public key encryption with symmetric key encryption for example, is not changing the principles of operation of Kessler, the requirement of the MPEP is simply rendered meaningless.

At page 42, the Examiner's Answer essentially asserts that encryption and obfuscation can be the same thing. This again goes against the level of skill in the art as established by the prior art references in the instant appeal. Kessler consistently distinguishes between what is obfuscation and encryption. Kessler provides a definition of obfuscation. See Kessler, Col. 8, lines 57, 58. Kessler treats encryption and being separate and distinct from encryption and teaches when each is needed. Nowhere does Kessler teach that obfuscation is associated with the track key and so taken as a whole teaches one of skill in the art that encryption of the track key is sufficient.

Yet again, the Examiner's Answer asserts that it is appropriate to modify the primary reference, treating encryption as obfuscation, in a way that directly contradicts the principles of Kessler which distinguishes between obfuscation and encryption. Since the interpretation given in the Examiner's Answer at page 42 contradicts Kessler, the interpretation changes the principles of Kessler. As previously quoted, under the as a whole analysis, the MPEP explicitly stated that such modifications are inappropriate and so should be given no weight. MPEP §2143.01 VI., 8th Ed., Rev. 6, pg. 2100-141, (Sept. 2007).

Finally, the primary reference teaches two distinct processes, one is providing software to each client for implementing peer-to-peer file transfer and the other process is two users actually implementing a secure peer-to-peer file transfer. The Examiner's Answer repeatedly asserts that the analysis in the Appeal Brief is confused. However, any confusion follows directly from trying to explain that the rejection takes unrelated pieces from the peer-to-peer file transfer and then uses the pieces in a totally different way. The source of the confusion continually referenced in the Examiner's Answer is the failure of the Examiner's Answer and

Serial No. 10/672,184
Examiner's Answer Dated: August 29, 2008
Reply Brief Filed: October 28, 2008

the rejection to consider Kessler as a whole, as required by the MPEP in an obviousness rejection. The Appeal Brief demonstrates that independent of what is selectively extracted and reassembled from the references, when consistent definitions are used the combination of references fails to support that interpretation used in the rejection.

Analyzing references, as was done in Appellant's Brief to determine whether the rejection changes the principles of operation of the reference taken as a whole is not attacking the references individually, but rather demonstrating that the rejection failed to do a proper analysis as required by the MPEP.

In conclusion, Appellant has explained at multiple levels why the combination of references fails to render the invention as recited in Claims 1 to 4, 6 to 9, 11 to 14 and 16 to 19 obvious. Thus, the Examiner's rejection of Claims 1 to 4, 6 to 9, 11 to 14 and 16 to 19 should be reversed.

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on October 28, 2008.



Attorney for Appellant(s)

October 28, 2008
Date of Signature

Respectfully submitted,



Forrest Gunnison
Attorney for Appellant(s)
Reg. No. 32,899
Tel.: (831) 655-0880